STATEMENT BY THE INDEPENDENT REVIEWER OF TERRORISM LEGISLATION ON PUBLICATION OF THE REPORT OF THE INVESTIGATORY POWERS REVIEW ('A QUESTION OF TRUST')

11 June 2015

EMBARGOED FOR USE AFTER THE REPORT IS LAID IN PARLIAMENT BY THE PRIME MINISTER ON THURSDAY 11 JUNE 2015

Today the Prime Minister published the Report of the Investigatory Powers Review, entitled 'A Question of Trust'. It was submitted to him by David Anderson Q.C. Independent Reviewer of Terrorism Legislation.

Quote

David Anderson said:

"Modern communications networks can be used by the unscrupulous for purposes ranging from cyber-attack, terrorism and espionage to fraud, kidnap and child sexual exploitation. A successful response to these threats depends on entrusting public bodies with the powers they need to identify and follow suspects in a borderless online world.

But trust requires verification. Each intrusive power must be shown to be necessary, clearly spelled out in law, limited in accordance with international human rights standards and subject to demanding and visible safeguards.

The current law is fragmented, obscure, under constant challenge and variable in the protections that it affords the innocent. It is time for a clean slate. This Report aims to help Parliament achieve a world-class framework for the regulation of these strong and vital powers."

The Report

The Review was conducted by a small independent team under the leadership of David Anderson Q.C. It received almost 70 written submissions. Further evidence was taken from public authorities (at the highest level of security clearance) and from a wide range of organisations and individuals in the UK, California, Washington DC, Ottawa, Berlin and Brussels.

Parts I-III of the Report (Chapters 1-12) inform the debate by summarising the importance of privacy, the threat picture, the relevant technology, external legal constraints, existing law and practice and comparisons with other types of surveillance, other countries and private sector activity. They also summarise the views expressed to the Review by law enforcement, intelligence, service providers and civil society.

Part IV of the Report (Chapters 13-15) sets out five underlying principles and 124 separate recommendations. Taken together, they form the blueprint for a new law to replace the Regulation of Investigatory Powers Act 2000 **[RIPA]** and the dozens of other statutes authorising the collection of communications data.

The ***key recommendations*** are summarised in paras 10-34 of the Executive Summary at the start of the Report. They include, in particular:

(a) a new law that should be both ***comprehensive*** in its scope and ***comprehensible*** to people across the world (Executive Summary, paras 10-11);

(b) maintaining, subject to legal constraints, existing capabilities relating to ***compulsory data retention*** as provided for by DRIPA 2014 and formerly under an EU Directive (ES, para 12);

(c) the enhancement of those capabilities (e.g. by requiring the retention of "***weblogs***" as proposed in the draft Communications Data Bill 2012, the so-called "snoopers' charter") only to the extent that a detailed operational case can be made out and a rigorous assessment has been conducted of the lawfulness, likely effectiveness, intrusiveness and cost (ES, para 13);

(d) the retention subject to legal constraints of ***bulk collection*** capabilities (the utility of which is briefly explained by reference to six case studies from GCHQ: Annex 9), but subject to additional safeguards and to the addition of a new and lesser power to collect only communications data in bulk (ES, paras 14-15);

(e) a new requirement of ***judicial authorisation*** (by Judicial Commissioners) of all warrants for ***interception***, the role of the Secretary of State being limited to certifying that certain warrants are required in the interests of national security relating to the defence or foreign policy of the UK (ES, paras 16-17);

(f) measures to reinforce the ***independence*** of those authorising requests for communications data, particularly within the security and intelligence agencies (ES, para 21);

(g) a new requirement of ***judicial authorisation*** of ***novel and contentious*** requests for ***communications data***, and of requests for privileged and confidential communications involving e.g. ***journalists and lawyers*** (ES, paras 25-27);

(h) the ***streamlining of procedures*** in relation to warrants and the authorisation of requests for communications data by local authorities and other minor users (ES, paras 19, 23-24);

(i) improved supervision of the ***use of communications data***, including in conjunction with ***other datasets*** and ***open-source intelligence*** (ES, para 29);

(j) maintaining the ***extraterritorial effect*** in DRIPA 2014 s4, pending a longer-term solution which should include measures to improve the cooperation of overseas (especially US) service providers and the development of a new international framework for data-sharing among like-minded democratic nations (ES, para 20).

(k) the replacement of three existing Commissioners' offices by the ***Independent Surveillance and Intelligence Commission***: a new, powerful, public-facing and inter-disciplinary intelligence and surveillance auditor and regulator whose judicial commissioners would take over responsibility for issuing warrants, for authorising novel, contentious and sensitive requests for communications data and for issuing guidance (ES, paras 28-32);

(l) expanded jurisdiction for the ***Investigatory Powers Tribunal***, and a right to apply for permission to appeal its rulings (ES, para 33); and

(m) the maximum possible ***transparency*** on the part of ISIC, the IPT and public authorities (ES, para 44).

Other Reports

- The Report endorses some of the recommendations of the ***Intelligence and Security Committee*** of Parliament ("Privacy and Security", March 2015). But the Report is broader in its scope, covering the activities of all 600 bodies with powers in this field and not just the security and intelligence agencies. It also departs from the ISC in recommending (a) that a new law should apply across the board (Report, 13.35-13.44), and (b) that interception warrants should be judicially authorised (Report, 14.47-14.57).

- A further Independent Surveillance Review, to be conducted under the auspices of the Royal United Services Institute (RUSI), was commissioned in March 2014 by the Deputy Prime Minister. It has not yet issued a report.

Encryption

- There has been some recent media speculation on the subject of encryption, which it may be useful to correct.

- The position communicated by the security and intelligence agencies to the Review is summarised (Report, 10.20) as follows:

> "The Agencies do not look to legislation to give themselves a permanent trump card: neither they nor anyone else has made a case to me for encryption to be placed under effective Government control, as in practice it was before the advent of public key encryption in the 1990s. There has been no attempt to revive the argument that led to the Clipper Chip proposal from the NSA in the 1990s, when public key cryptography first became widely available. But the Agencies do look for cooperation, enforced by law if needed, from companies abroad as well as in the UK, which are able to provide readable interception product."

- The Report recommends that in the digital world as in the real world, "*no-go areas*" for intelligence and law enforcement should be minimised (13.7-13.14). But as concluded at 13.12:

> "Few now contend for a master key to all communications held by the state, for a requirement to hold data locally in unencrypted form, or for a guaranteed facility to insert back doors into any telecommunications system. Such tools threaten the integrity of our communications and of the internet itself. Far preferable, on any view, is a law-based system in which encryption keys are handed over (by service providers or by the users themselves) only after properly authorised requests."

Notes for editors:

Section 7 of the Data Retention and Investigatory Powers Act 2014 http://www.legislation.gov.uk/ukpga/2014/27/section/7/enacted required the Independent Reviewer of Terrorism Legislation to examine:

a) the threats to the United Kingdom;
b) the capabilities required to combat those threats;
c) the safeguards to protect privacy;
d) the challenges of changing technologies; and
e) issues relating to transparency and oversight;

and to report to the Prime Minister on the effectiveness of existing legislation relating to investigatory powers, and to examine the case for a new or amending law. This Report is a result of his work on those issues.

David Anderson Q.C. is a barrister practising from Brick Court Chambers in London, a Visiting Professor at King's College London, a Judge of the Courts of Appeal of Guernsey and Jersey and a Bencher of the Middle Temple. He is an experienced advocate in the European Court of Human Rights and in the Court of Justice of the EU: http://www.brickcourt.co.uk/people/profile/david-anderson-qc. He has served on a part-time basis since 2011 as the Independent Reviewer of Terrorism Legislation, reporting in that capacity to the Home Secretary, to the Treasury and to Parliament on the operation of the UK's anti-terrorism laws.

Contact:

For more information about the Independent Reviewer of Terrorism Legislation and for a full copy of the Report please go to: https://terrorismlegislationreviewer.independent.gov.uk or contact his clerk kate.trott@brickcourt.co.uk. You can also follow David on Twitter: @terrorwatchdog